Patient Privacy Preservation: P-RBAC vs OrBAC in Patient Controlled Records Type of Centralized Healthcare Information System. Case study of Walloon Healthcare Network, Belgium

Annanda Thavymony Rath
Faculty of Computer Science
University of Namur, Namur, belgium
Email: rta@info.fundp.ac.be

Jean-Noël Colin
Faculty of Computer Science
University of Namur, Namur, belgium
Email: jnc@info.fundp.ac.be

***Abstract*—This paper addresses the issue of access control to sensitive data in the health sector. Our work aims to identify a suitable access control model based on specific access requirements and constraints for Patient Controlled Records type of Centralized Healthcare Information System, particularly, Walloon Healthcare Network. Two prominent access control models are considered, Privacy-aware Role Based Access Control and Organization-based Access Control. In this paper, we outline the access control requirements and based on those requirements, we apply, compare, and point out the advantages and disadvantages of the two models.**

***Keywords*-Access Control; Privacy Preservation; e-health; P-RBAC; OrBAC; Patient controlled record.**

I. INTRODUCTION

E-Health provides significant opportunities for healthcare institutions to deliver technologically effective services to their patients. With the online availability of health record, healthcare professionals can make use of it in health service, for instance, an emergency situation where health record history is required in order to provide a safe and effective treatment. However, the major concern in e-health is security; as data is available online, it is vulnerable to attacks. Failing to secure this type of information can lead to huge fines, lawsuits, or long-term loss of patients' trust. Yet to provide adequate security, in a manner that is not burdensome to patient can be a major challenge.

Many researches [1][4][5][6][7][9][12] have been conducted in the aspect of privacy preservation in e-health, particularly, access and usage control. In general, access control refers to the cautious actions/measures that need to be taken before data is liberated while usage control refers to the actions/measures taken after data is granted access. In the data protection point of view, specially, privacy-related environment, the enforcement of the two controlling steps is necessary. Concerning to access control, many models are available [3][13], however only a few of them are proposed so far in e-health literatures such as RBAC [3], P-RBAC (Privacy-aware Role-based Access Control) [7], OrBAC [2] and the workflow-based [4]. Every model has its own strengths and weaknesses and it suits to different access requirements and constraints. Thus, it is important, when building an e-health system, to identify and study different access control models before adopting it.

This paper provides a study of two prominent access control models P-RBAC and OrBAC. Our main goal is to identify an appropriate access control model that can be adopted to preserve and protect patient's health record in patient controlled health records type of centralized healthcare information system(PCRCHIS), particularly, Walloon Healthcare Network(WHN) [1][10]. The complexity of policy expression, evaluation, and the ability to fulfill the system requirements are our main comparison parameters. The rest of this paper is organized as following.

Section II is an introduction to Walloon Healthcare Network and its access requirements and constraints. Section III talks about some standard access control models. Section IV introduces the P-RBAC and OrBAC models. Section V is about applying P-RBAC and OrBAC in WHN. Section VI talks about the advantages and disadvantages of the two models, and Section VII is the conclusion and future work.

II. WALLOON HEALTHCARE NETWORK

Walloon refers to the French speaking region in Belgium. Walloon Healthcare Network (WHN) [1] is a project aiming to provide an electronic healthcare facility to patients in Walloon region by joining together all healthcare institutions, clinics, and also physicians and allow exchanging patient's record when needed.

A. System Architecture

As illustrated in Figure 1, WHN is a network of health institutions such as hospitals, and clinics, but also of physicians that aims at supporting the exchange of patient's data between healthcare professionals, in a timely and secure way. WHN is organized as a hub that interconnects all entities, and provides central storage. Two types of data are actually stored centrally:

- pointers to EHR(Electronic Health Record) stored in institutions.
- SumEHR(Summarized Electronic Health Record) which is a summary record maintained by the

 ISBN: 978-1-61208-179-3

physicians.

Thus, WHN provides indexes to data that resides in network nodes (healthcare institutions), but does not store that data itself. In addition, WHN also manages in a central way the access permissions that apply to various pieces of data it manages (indexed data as well as SumEHR). WHN central server is in charge of the overall authorization process; it receives requests from the nodes, checks them against the applicable access policy, and returns the requested information. For more details, refer to [1].

WHN adopts the PCRCHIS like architecture, which refers to a system where management and control of access rights are performed by patient or trusted person. It has two important aspects. First, patient controlled record [8] refers to a system where management and control of access are performed by patient or patient's trusted-person. In this system, patient can grant access to anyone they wish and role of healthcare institution in controlling patient's record is minor and their responsibility is only to secure the storage of patient's health record. Second, centralized system [8] refers to a large network of healthcare institutions such as hospitals or clinics join together locally or regionally with one central point of access control. Thus, the access requirements in PCRCHIS are not as simple as that of the standalone system(system used particularly in a specific healthcare institution). The main issues in this system are:

1) Interoperability: How to ensure that the policies/rules defined in one healthcare institution are understood by other in the network.
2) Access and Usage: How to protect patient's record when it is shared across different healthcare institutions. In this system, data is exchangeable between different institutions. Thus, we need a proper mechanism to ensure that the same level of protection is assured while it is at the destination or moved out.
3) Patient's knowledge and policy management: In this system, patient has the pivotal rights to grant access and manage the access policies over their health records. It is understood that, not all users have the required computer skills, it is really hard to assume that user has the sufficient knowledge to administrate the access policy by themselves. In this case, the careful design of policy administration point is an important task in order to response to or cope with the errors made by patient. In addition, the rule validation and conflict resolution should be also carefully addressed.

B. Access Requirements and Constraints

This section presents the requirements and constraints needed to access patient record in WHN. Through WHN's specification [1], we can identify the requirements as following:

1) In this system, patient's record can be accessible by five types of user:s Users in role generalist-doctor, specialist-doctor, emergency-doctor, guardian, and trusted-person. Guardian, a person closed to patient who can represents patient in case he/she can not exercise his/her rights, for instance, parents can be a child's guardian if child's age is below 18. Trusted-person is a user or group of users, assigned by patient, who can decide instead of patient when patient is in situation where he/she can not exercise his/her rights physically or morally. In general, trusted-person can be patient's wife, husband, or parents.
2) Requester has the therapeutic relationship with patient. This relationship is defined by patient. Therapeutic relationship is an indication of the relation between requester and patient.
3) Accessing patient's record is subjected to patient's consent. And consent can be revoked any time.
4) Patient can grant access to his/her record and the rights assignment can be done by patient or through the support of the guardian, trusted-person, or healthcare professional. In any case, the assignment requires patient's consent. It is important to note that patient can also transfer the rights to guardian or trusted-person in case patient can not exercise his/her rights. For example, in case patient becomes mentally disable.
5) Every access to patient's record, requester needs to notify, this is considered as an obligation.
6) Access to patient's record is allowed for a specific purpose. There are three types of purpose. **Personal archive**: It is generally related to patient. It is allowed in case he/she wants to consult his/her health record. **Normal**: it is granted to doctor for normal health examination. **Emergency**: It is granted only to doctor in emergency situation. It is important to note that patient needs to define in advance the access policy in case of emergency situation. Patient can allow the selected groups of doctor or all doctors to access his/her health record.

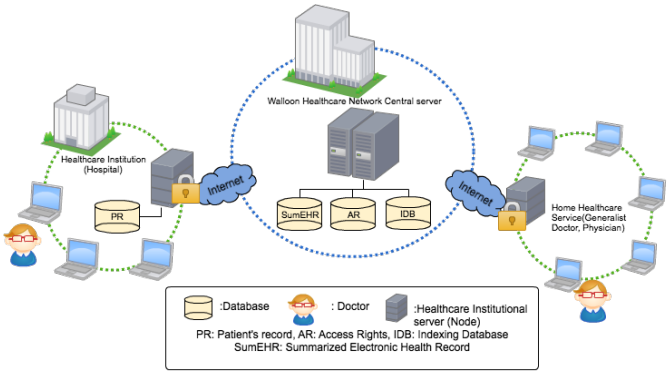

Figure 1. Simplified Schema of Walloon Healthcare Network

With the above requirements, we can identify the general rules to access patient's record as following. Requester is

granted access to patient's record if:

- **Rule-1:** Requester is in one of the five user groups as mentioned above.
- **Rule-2:** Requester has therapeutic relationship with patient and patient's consent .
- **Rule-3:** Requester fulfilled their duty or obligation such as notifying system for traceability.
- **Rule-4:** Access purpose falls into three types of purpose mentioned above.

III. Standard Access Control Models

In this section, we outline some standard access control models such as DAC, MAC, and RBAC. And based on the requirements in Section II, we point out why they are not suitable for the proposed system.

Discretionary Access Control (DAC) [3][13] is an access control model where restriction of access to objects is done based on the identity of subjects. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to any other subjects. For example, an access control to files and folders in Unix system where user can define permission for other users to access their file or folder is a clear example of DAC. One implementation of DAC is the access control list that has been used widely in operating, networking, and database management system.

Although the ability of passing access permission on to any other subjects seems to match with the requirements in PCRCHIS, DAC fails to fulfill other important requirements such as the ability to express complex permission assignment that involves purposes, obligations and conditions, which are the most important elements for expressing the privacy-related policy. Moreover, DAC can not support data and role hierarchy expression which is required in PCRCHIS for data as well as user management. For example, the classification of generalist-doctor to many sub-groups according to their speciality/skill such as a doctor specializing in liver, nose, heart, and so on. This proves the necessity of role hierarchy. In addition, DAC has the problem of controlling the permission transfer and policy change, which are required in the proposed system (Section II(B) requirement 4), for instance in case of guardian or trusted-person. In order for the guardian or trusted-person to be able to represent a patient, a patient needs to define the permission transfer, which is considered as the legal binding document. Another draw back of DAC is the ability to express the separation of duties.

Mandatory Access Control(MAC) [3][13] is used widely in the operating system, databases, and networking system. MAC refers to a type of access control model by which the system constrains the ability of a subject or requester to access or perform some sort of operation or action to an object or resource. In practice, the subject refers to an entity that can be a user or application; object refers to the files, directories, ports (in networking), or databases (tables or attributes in database management system). In MAC, subjects and objects each have a set of security attributes and when a subject makes an attempt to access an object, an authorization rule enforced by the system examines these security attributes and then the decision can be made whether the access can take place. To determine if the operation on the object by a subject is allowed or not, those parameters will be tested against the set of the authorization rules made by the policy maker or administrator of the system. MAC provides the central control of the security. User or subject does not have the rights to assign or override the policy unlike ACL, which allows subject to make decision or override the access policy. MAC provides more control level compared to ACL as both subject and object carry the secured attributes that need to be checked or tested by system for every access attempt.

The disadvantage of MAC lies in the complexity of the configuration, since for each resource (application, data) and subjects (user) must be determined, which access authorizations are necessary. This tends to be very difficult for the system that works with the large number of users and resources, particularly, in system like PCRCHIS(refer to its definition in Section II). Another down part is that MAC is not designed to enforce privacy policies and barely meet privacy protection requirements, particularly, purpose binding (i.e. data collected for one purpose should not be used for another purpose without user consent), conditions and obligations. The purposes and obligations are a part of the requirements in PCRCHIS. Purposes are not only used to sharpen the access control but also to enforce the security protection in case of emergency situation. Additionally, MAC can unnecessarily over-classify data through the high-water mark principle and hurt productivity by limiting the ability to transfer labeled information between systems. This would be a great disadvantage for PCRCHIS.

Role-Based Access Control(RBAC) has been introduced in many research literatures [3][5][7][8]. The authors address the issue of protecting patient record by restricting access based on user's role and in this model, users who are in the same role can exercise the same level of rights. With this classification, access control on patient's record can be realized only with the simple access policy as access permission depends strongly on the role. However, it is hard to realize a complex and fine-grain access policy, particularly, in the contextual environment. For example, system that needs to differentiate access levels in the same role (requirement number 2 in Section II(B)), and most importantly, system that needs to express obligations or purposes (the requirements number 5 and 6 in Section II(B)). To complement this weakness, a context-awareness and privacy-awareness have been proposed [7]. In accordance with the spirit of the RBAC model, context-awareness or privacy-awareness RBAC(P-RBAC), access permission is granted to

 ISBN: 978-1-61208-179-3

user based not only on user role but also on the result of the occurrence events in the system or purpose of access. The context can be anything ranging from spatial, temporal to user pre-defined context. This new approach offers rich, fine-grain and flexible way to express the privacy-related policies, particularly, in the proposed system.

The authors realize the privacy-awareness by adding other entities to the core RBAC model such as conditions, obligations, and purposes of access. It is important to note that although standard RBAC can not express the obligations, purposes, and conditions, it has the ability to provide many features that are necessary for expressing access policy in WHN such as the ability to express data and role hierarchy, permission transfer as well as separation of duties. More details can be found in Section IV.

In June 2003, Abou and Baida proposed OrBAC [2] for healthcare application domain. With OrBAC, the access permission is granted to user under a specific role in particular organization and contexts. A user in one healthcare institution can access data to another institution if and only if the permission is granted by those institutions. This provides data integrity and confidentiality. OrBAC supports the control of data as well as user in system like organization structure and access permission is granted based on user role in an organization. In addition, it can also express the access permission in contextual environment, role and data hierarchy, separation of duties as well as permission transfer, which perfectly matches in WHN's requirements. Based on the requirements in Section II. We find that among the five models, OrBAC and P-RBAC are the most appropriate models. More discussion can be found in Section VI.

IV. P-RBAC AND ORBAC

This section presents a brief introduction to P-RBAC and OrBAC to provide the fundamental knowledge for model expression that is required in the next section.

A. Privacy-Aware Role-Based Access Control Model

P-RBAC [7] is an extension of the model RBAC [3], which provides complete support for expressing highly complex privacy-related policies. Its focus is to protect personally identifiable information and as such privacy-sensitive, taking into account characteristics such as goals (purposes), conditions, and obligations. P-RBAC extends the classical RBAC by adding three more privacy-related entities such as purposes, conditions, and obligations.

As shown in Figure 2, P-RBAC consists of the following entities: **Users** represent human or the interactive entity. **Roles** represent a function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member's role. **Data** refers to all resources related to an organization or individual identified or identifiable. **Actions** are the operations on resources; action varies depending on the content and format. **Purposes**, in P-RBAC, permissions are assigned to roles and users for a specific purpose. **Conditions** are the mechanisms to precisely define the authority over resources to a specific role; using condition, we can express different access rights for user in the same role. **Obligations** are the necessary actions to be made before the actions on content can be exercised.

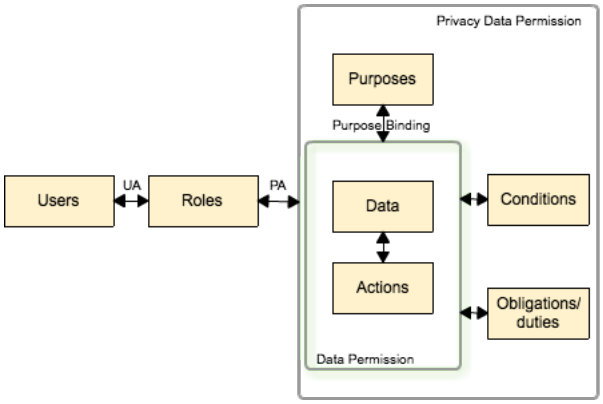

Figure 2. P-RBAC Entities Model

1) P-RBAC definition and rule formulation

- U is a set of users (u); D is a set of data (d); A is a set of actions (a); Pu is a set of purposes (pu); Ob is a set of obligations (ob); R is a set of roles (r)
- LC: condition language; PA: permission assignment
- Data Permission (DP): DP = $\{(a,d) \mid a \in A, d \in D\}$
- Privacy-sensitive Data Permission (PDP): PDP = $\{(dp, pu, c, ob) \mid dp \in DP, pu \in Pu, c$ is a expression of LC, $ob \in Ob\}$.
- PA on a role is defined as: **PA: (r, ((a,d), pu, c, ob)))**
- User Assignment UA $\subseteq U \times R$ (many to many relations)
- Privacy-sensitive Data Permission Assignment PDPA $\subseteq R \times PDP$

2) The Basic Condition Language

Core P-RBAC [7] includes a simple language for expressing conditions; they are expressed using contextual variables. Such variables record privacy-related information that is to be taken into account when enforcing privacy permissions. Contexts range from temporal, spatial to the pre-defined context by user. It is important to note that the condition expression here is defined in such a way so that it can be served to model several conditions usually found in privacy permission. The conditions that can be expressed by LC are defined in what follows.

Definition: Let X be a set of contextual variables(CV); each variable $x \in X$ has a finite domain of possible values, denoted as Dx; every domain is equipped with a pair of corresponding relational operators $\{=, \leq, \geq, \neq, \ni\}$. An atomic condition ac defined over X has the form (x opr v) where $x \in X$, $v \in Dx$, opr $\in \{=, \leq, \geq, \neq, \ni\}$. The

conditions of LC (over X) are defined as follows:

- An atomic condition is a condition of LC.
- Let ci and cj be conditions of LC; then ci ∧ cj is a condition of LC.

3) The Basic Obligation Model

An obligation is the duty for subject to fulfill before access is granted. An obligation may be different depending on context and system environment. For example, a system that serves online song or music, obligation may be a payment while in healthcare information system, obligation can be a notification of access to patient for traceability purpose. To simplify the problem we focus on one typical example of obligation, which is notification to data owner after each access to his/her sensitive data. we formalize our obligation as a ”notify” function . The function takes an email address of content owner and acknowledgement message as the inputs and returns ”yes or no” statement as an output in case of success to notify and fail to notify respectively. Thus, our obligation function can be written: **notify(patient's email, notified_message)**.

B. Organization-Based Access Control Model (OrBAC)

OrBAC [2] allows expressing a variety of security policies based on the concept of organization. The main goal of OrBAC is to allow the policy designer to define a security policy independently from the deployment. The chosen method to fulfill this goal is the introduction of an abstract level in the model. OrBAC model is based on three principles: organization, concrete and abstract level, and context. Organization is an entity that each security policy is defined for. Like other models, concrete authorization in OrBAC relies on three entities, which are subject, action, and object. Subject is an interactive entity, user or application that requests access on the organization's object. Action is an operation on object. Object is a resource requested by subject. In OrBAC, a concrete authorization is derived from abstract permission, which consists of three entities such as role, activity, and view. Role represents a function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member's role. Activity groups actions into an abstract set and view is a set of abstract objects.

Typically, as presented in Figure 3, a subject in concrete level is mapped to a role in abstract level where an action is mapped to an activity and an object is mapped to a view. OrBAC has many advantages, in addition to its ability to express the permission; it can also express a mixed policy with permissions, prohibitions, and obligations. With OrBAC, security policies could take into account delegation, hierarchy, and context [11]. There are five categories of context: **temporal**, **spacial**, **context declared by the user**, **prerequisite Context**, and **provisional context**.

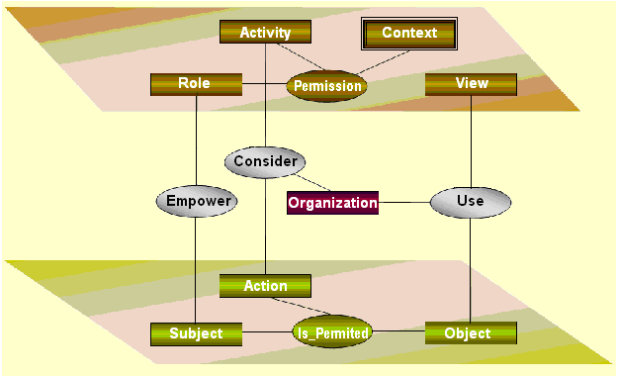

Figure 3. OrBAC Entities Relationship Schema

1) OrBAC definition and rule formulation

In this section, we present a mean of representation and reasoning about the permission, prohibition, and obligation in given of the entities, Subject, Action, Object, Role, Activity, and View.

1. Abstract expression (Permission, Prohibition, or Obligation) indicates an authorization, prohibition, or obligation of an organization allowing user under a specific role to perform an activity on a view that is considered by and used in an organization. This authorization is constraint with a specific contextual attributes if presented . They are expressed as following:

- Permission(Organization,Role,Activity,View,context)
- Prohibition(Organization,Role,Activity,View,context)
- Obligation(Organization,Role,Activity,View,context)

2. Concrete expression (Permission, Prohibition, or Obligation) indicates an authorization, prohibition, or obligation of an organization for a specific user to perform a requested action on requested object. It is important to note that concrete permission, prohibition, or obligation is derived from the abstract level expression and can be expressed as following:

- Is_permitted(Subject, Action, Object)
- Is_prohibited(Subject, Action, Object)
- Is_obliged(Subject, Action, Object)

3. Deriving concrete permission: It is important to note that in order to get the concrete permission from abstract level, we have to pass a few verification processes such as to verify if subject is in role, action is in activity, and object is in view, which are allowed in abstract permission. The expressions can be written as following.

- Empower (Organization, Subject, Role): Organization assigns a role to subject(user).
- Use (Organization, Object, View): Organization uses an object in a view.
- Consider(Organization, Action, Activity): Organization considers an action in an activity.

In case contexts are represented, the concrete permission can be achieved if and only if all contextual attributes are

checked and they hold together subject, action and object.

- Hold(Organization, Subject, Action, Object, Context)

V. APPLYING P-RBAC AND ORBAC

In this section, we express the access rules applied in WHN by using P-RBAC and OrBAC based on an access scenario below. It is important to note that in order to avoid confusion when comparing the policies expression of the two models. We term them as following: $Rule1_{P-RBAC}$ is used for P-RBAC to express the access rule "1" in P-RBAC and $Rule1_{OrBAC}$ is used for OrBAC to express the access rule 1 in OrBAC. We define variables, values, and functions used in P-RBAC and OrBAC as following:

1) P-RBAC: Roles (R)= { Specialist-Doctor}; Objets (O) = {Liver_report}; Actions (a)= {read}; Purposes (PU)= { Norma, Emergency}; OB={Notity}; N/A= not available;
2) OrBAC: Orgs = { CSL, CHN } Where CSL= Clinic Saint Luc, CHN = Central Hospital of Namur; Users(U)(Subjects) = {Alice, Charlie, Pierre}; Roles (R)= {Specialist-Doctor}; Objets (O) = {Liver_report}; Activities (av)= {Consult, Notify}; Actions (a)= {read, send}; Views = {Health records}; Purposes (PU)= { Normal, Emergency}; OB={Notity}; ANY_org= represents any organization.

Supposing that an object as data and object as person are merged into a single entity called "object". Then we are able to refer object.role to identify the role of data owner in this case patient; object.ehr for health record; object.consent refers to a list of consented users; object.email refers to email address of patient; object.therapeutic_ relationship refers to list of users who have the relationship with patient; object.ar refers to access record. Supposing that subject is a user who initiates request then subject.id is user identification; subject.role is role of requester(subject); subject.pu refers to purpose of access; subject.in refers to institution that subject belongs to.

A. Scenarios Description

Supposing that there are two institutions joining WHN, one is CSL and other is CHN. Charlie is a specialist doctor at CSL and CHN while Pierre is a specialist doctor at CHN only. Alice has registered as a patient in WHN. Alice has declared her Liver_report in WHN. Alice assigned Charlie and Pierre as her "Specialist-Doctor". Alice would like to set the access rights on her dossier as following:

- Rule 1: User in role Specialist-Doctor can read Alice's Liver_report if: Data being requested is belong to Alice; and user has therapeutic relationship with Alice; and user has Alice's consent; and purpose of access is for emergency situation; and the notification of access is fulfilled.
- Rule 2: Alice would like to give consultation(read) permission to Specialist-Doctor on her Liver_report only when requester is working under institution different from CSL for the purpose of normal treatment, but every accesses, he/she has to notify system. It is important to note that Rule 1 is included in Rule 2. The differences between rule 1 and 2 are purpose and the introduction of another access requirement which is the location(institution) from which the request is initiated.

B. Apply P-RBAC

$Rule1_{P-RBAC}$: (Specialist-Doctor,((Read, object.Liver_ report), subject.pu=Emergency, object.role=patient $\wedge$ object. therapeutic_relationship $\ni$ subject.id $\wedge$ object.consent $\ni$ subject.id, notify(object.email, notify_message)=yes))

$Rule2_{P-RBAC}$: (Specialist-Doctor,((Read, object.Liver_ report), subject.pu= Normal, object.role = patient $\wedge$ object.therapeutic_relationship $\ni$subject.id $\wedge$ object.consent $\ni$ subject.id $\wedge$ subject.in$\neq$"CSL", notify(object.email, notify_message)=yes)))

C. Apply OrBAC

$Rule1_{OrBAC}$**: abstract permission and obligation**
Permission(ANY_org,Specialist-Doctor,Consult,object. Liver_report,object.role=patient $\wedge$ object. therapeutic_relationship $\ni$ subject.id $\wedge$ object.consent $\ni$ subject.id $\wedge$ subject.pu = Emergency).
Obligation(ANY_org, Specialist-Doctor, Notify, object.ar, object.role = patient $\wedge$ object.therapeutic_relationship $\ni$subject.id $\wedge$ object.consent$\ni$subject.id $\wedge$ subject.pu = Emergency).

$Rule2_{OrBAC}$**: abstract permission, obligation, and prohibition**
Permission(ANY_org,Specialist-Doctor,Consult,object. Liver_report, object.role=patient $\wedge$ object.therapeutic _relationship$\ni$ subject.id $\wedge$ object.consent$\ni$ subject.id $\wedge$ subject.pu= Normal)
Obligation(ANY_org, Specialist Doctor, Notify, object.ar, object.role=patient $\wedge$ object.therapeutic_relationship$\ni$ subject.id $\wedge$ object.consent$\ni$ subject.id $\wedge$ subject.pu= Normal)
Prohibition(CSL,Specialist-Doctor,Consult,object. Liver_report, object.role=patient $\wedge$ object.therapeutic _relationship$\ni$ subject.id $\wedge$ object.consent$\ni$ subject.id $\wedge$ subject.pu= Normal)

VI. DISCUSSION

In WHN, access permission to medical record is based on requester role, relationship between requester and patient, patient's consent, purpose of access, and obligation. In addition, patient can also restrict access by using spatial or temporal context such what has been illustrated in rule 2 Section V (B,C). Based on the illustration in Section V, we

 ISBN: 978-1-61208-179-3

find that OrBAC can be used but not really appropriate for this system.

First, in WHN, the entity organization(institution) does not play an important role in access policy, it is required only in the indexing process and later it is considered as the link to content. The impertinent role of entity organization can be seen clearly in the scenario where patient grants access to guardian or trusted-person(they, as presented in Section II, are not necessary the users under any institutions). This access scenario shows that the organization entity does not play an important role at all in access policy. The organization may be of course used to restrict access, but in this case it can be considered as a conditional attribute as illustrated in P-RBAC (Section V(B), $Rule2_{P-RBAC}$).

Second, as illustrated in Section V, we found that using OrBAC in the scope of WHN is more complex than using P-RBAC. Let compare rule $Rule2_{P-RBAC}$ and $Rule2_{OrBAC}$ in Section V(B) and V(C) respectively: Using P-RBAC, as illustrated in rule $Rule2_{P-RBAC}$, we can express the access rights in a single rule where the organization entity (considered in OrBAC) becomes simply as a conditional attribute (subject.in). $Rule2_{P-RBAC}$ expresses the rights for all users in role Specialist-Doctor, but it restricts access from a particular IN (Institution), CSL as an example. in OrBAC with the same scenario, we need to have three rules. One applied to permission while other applied to obligation and prohibition. In the data processing point of view, time required to process or evaluate $Rule2_{OrBAC}$ is more than that of Rule2$_{P-RBAC}$.

To make it clear for the second remark, let us take a scenario (rule 2) where Alice sets a new policy in which she prohibits users from two particular institutions, this time CSL and CHN, to access her Liver_report. In this case, if we express it by using P-RBAC, we still use one rule by having one more condition on institution (subject.in$\neq$"CSL" $\wedge$ subject.in$\neq$"CSL") while with OrBAC we need four rules, one for permission, one for obligation and other two for prohibition(CSL and CHN). Although concept of grouping for organization entity can be used in OrBAC, in case of prohibition, it consumes time in policy evaluation process.

In WHN, obligation and purpose of access are required, both models can provide these features. In P-RBAC, both obligation and purpose can be expressed in the permission assignment. In OrBAC, obligation is expressed in the separate rule(Section V (C)) while purpose can be considered as the contextual attribute as illustrated in Section V(C) (rule $Rule1_{OrBAC}$). For prohibition, in OrBAC, it can be expressed by using a separate rule($Rule2_{OrBAC}$) while in P-RBAC it can be expressed in condition or using a negative permission expression [7].

In either way, expressing access policy by using OrBAC in the scope of WHN is seen as less suitable and more time-consuming in policy evaluation process as compared with P-RBAC, especially when obligation and prohibition are involved. Based on above explanation, we can say that the two models can be adopted in WHN but the most appropriate one is P-RBAC. This conclusion is done based on four important points:

- In WHN or patient controlled records healthcare information system, in general, the entity organization does not play a significant role in the access policy, in some access scenarios(guardian and trusted-person), patient can grant access to anyone he/she wishes regardless of the institution they belong to. This proves the impertinent of entity organization in access policy.
- OrBAC is an organization based access control model where user must be strictly attached to organization. This does not fit well for the roles legal representative(guardian) and trusted-person(refer to Section II) because the two roles can be an independent role in the system and not under any institution where patient's record is stored.
- OrBAC is not specifically designed for privacy-aware. It is created for expressing access policy to control the resource in the system that adopts user management pattern like organization structure while P-RBAC is proposed for privacy-aware that fits well with the requirements in healthcare information system such as the WHN.
- Referring to the examples in Section V(B) and V(C), we found that expressing access policy by using P-RBAC can have a better response time(the proof of policy complexity can be seen by the number of attributes and operations in rules and the rules in policy) as compared with OrBAC, in other words, less time-consuming in evaluation process. This is because P-RBAC's policy contents less rules as compared with that of OrBAC.

VII. Discussion on some security issues

In this section, we discus about three security issues: rule validation, rule conflict detection and resolution, and security in case of emergency situation(breakglass).

A. Rule validation

In system where access control is based on rule, it is required for rule(access rule or policy) administrator to have the knowledge on how rule works and to be beware of what they are doing and the consequence of doing it. Under the scope of WHN or PCRCHIS in general, it is understood that it is not possible to make an assumption that all patients have sufficient computer skill or knowledge and can operate or set rule by themselves. Thus, to solve this problem, under the scope of WHN, the rule validation can be done by three groups of user:

1) Patient(record owner): Patient can set up the rule through policy administration point by themself without the support from healthcare professional or other

people such as their trusted-person or guardian(refer to its definition in Section II(B)), but if the problem occurs, for instance, patient mistakenly defines a rule that is not like what he/she wishes, it is the responsibility of patient themself.

2) Patient's trusted-person and guardian: In WHN, it is required for a patient to assign her trusted-person and/or guardian to represent them in case patient can not exercise his/her rights. Those person can help patient in setting up and validating the rule if patient wishes to do so.
3) Healthcare professional: In WHN, healthcare professional can also help patient to set the rule on their behalf, but patient's consent written in paper is required in this case.

B. Rule conflict detection and resolution

In P-RBAC, conflicting rules can be detected automatically by using conflict detection algorithms proposed by Qun Ni and Bertino in [7]. The conflict detection algorithms allows user to detect the conflict between rules(P-RBAC rules) and provides an alert to user for correction.

C. The security issue in case of emergency situation

In e-health, emergency access to patient's record in case of critical event such as emergency treatment is a major concern. The trade off between security and safety of patient must be carefully balanced. In WHN, we use a predefined rule in case of emergency situation. Patient needs to decide by themself about the access rights in case of emergency. He/she can allow user in role "emergency-doctor"(refer to Section II) to access their record for the fixed purpose(emergency). However, every access user needs to notify patient for traceability purpose. Note that in emergency situation, normal rules applied to required patient record are revoked and rule in case of emergency is applied.

VIII. Conclusion and future work

In this paper, we identified the access constraints and requirements for WHN based on the specification and privacy regulation of WHN. We also present two prominent access control models, P-RBAC and OrBAC. An access scenario with multiple rules is used to illustrate the performance of both models. Based on the discussion in Section VI, we conclude that in e-health system where role of organization is less important, for example, PCRCHIS. P-RBAC is the best candidate to be used if the complexity of policy expression and evaluation are the major concerns. It is important to note that although this paper is primarily the result from the study of WHN, we can also apply it in other systems having similar requirements and system architecture to WHN. Our future work includes the design of a platform based on P-RBAC allowing to create and to evaluate the rules/policies in PCRCHIS by taking WHN as the real case study. ODRL will be used as the default rights expression language.

References

[1] Espace dévelopeur de RSW (Development of WHN): https://www.reseausantewallon.be/developpement/default.aspx, latest access: July 2011.

[2] A.Bou, R. Baida, P.Balbiani, S.Benferhat, F.cuppens, and Y.Deswarte. Organization Based Access Control Model. 4th IEEE International Workshop on Policies for Distributed Systems and Networks, June, 2003.

[3] D.F.Ferraiolo, R.Sandhu, S.Gavrila, D.R.Kuhn, and R.Chandramouli. Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security, August 2001, pp.4(3):222-274.

[4] Giovanni Russello, Changyu Dong, and Naranker Dulay. A Workflow-Based Access Control Framework for e-Health Applications. Advanced Information Networking and Applications Workshops, 2008, pp.111-120.

[5] Hung, Patrick C. K, and Zheng Yi. Privacy Access Control Model for Aggregated e-Health Services. Proceedings of the 2007 Eleventh International IEEE EDOC Conference Workshop. IEEE Computer Society, pp.12-19.

[6] Lorenzo D. Martin, Qun Ni, Dan Lin, and Elisa Bertin. Multidomain and Privacy-aware Role Based Access Control in e-Health. Second IEEE International Conference on Pervasive Computing Technologies for Healthcare, Jan-Feb 2008, pp. 131-134.

[7] Qun Ni, Bertino, Elisa, Lobo, Jorge, Brodie, Carolyn, Karat, Clare-Marie, Karat, John, Trombeta, and Alberto. Privacy-aware Role-Based Access Control. ACM Transaction Information and System Security, July, 2010, pp.24-3.

[8] Rostad and Lillian. An Initial Model and a Discussion of Access Control in Patient Controlled Health Records. Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computer Society, pp. 935-942.

[9] Al-Neyadi, Fahed, Abawajy, and Jemal H. Context-Based E-Health System Access Control Mechanism. Advances Information Security and Its Application, Communications in Computer and Information Science, Springer Berlin Heidelberg, 2009, pp.68-77.

[10] Règlement relatif à la protection de la vie privée (Regulations for the Protection of User Privacy), Version 06h100809. https://www.reseausantewallon.be/Documents%20partages/R%C3%A8glement%20Vie%20Priv %C3%A9e.pdf, 2009, latest access: July 2011.

[11] Frédéric C and Nora.C. Modeling Contextual Security Policies in OrBAC. International Journal of Information Security (IJIS), August, 2008, pp. 285-305.

[12] Suzanne Gonzales-Webb and Craig M. Winter. HL7 Role-Based Access Control (RBAC) Role Engineering Process. HL7 Security Technical Committee, September 2007.

[13] Vincent C. Hu, David F. Ferraiolo, and D. Rick Kuhn. Assessment of Access Control System. National Institute of Standards and Technology, September 2006.

 ISBN: 978-1-61208-179-3